Field	Content
CERTIFICATE SERIAL NUMBER	UP TO THE MANUFACTURER. Eg. THE DEVICE SERIAL NUMBER (ICC ID) COMBINED WITH A KEY NUMBER.
ISSUER	MANUFACTURER IDENTIFICATION. Eg. THE SAME VALUE AS IN PKCS15TOKENINFO.MANUFACTURERID
VALID NOT BEFORE	DATE AND TIME OF CREATING/STORING THE KEY AND CERTIFICATE
VALID NOT AFTER	END OF EXPECTED MAXIMUM LIFETIME OF THE DEVICE
SUBJECT	A CONCENTRATION (STORED AS PRINTABLE STRING) OF • SERIAL NUMBER (ICC ID), SAME AS PKC215TOKENINFO.SERIALNUMBER • A LETTER (OR COMBINATION OF LETTERS) INDICATING KEY USAGE (PRECEDED WITH '-') • OPTIONALLY KEY ORDINAL NUMBER (PRECEDED WITH '-') Eg. 123456789O123456789-SD-2 9876543210987654-N
PUBLIC KEY	PUBLIC KEY ASSOCIATED WITH THE PRIVATE KEY IN THE DEVICE

FIG. 1a

KEY USAGE INDICATOR	SUPPORTED WIM PRIMITIVES WITH THIS KEY	COMMENT
N	COMPUTERDIGITALSIGNATURE	NON-REPUDIATION. THE WIM REQUIRES USER VERIFICATION (PIN) EVERY TIME
S	COMPUTERDIGITALSIGNATURE	DIGITAL SIGNATURES USED FOR AUTHENTICATION (E.g. FOR WTLS RSA OR SSL HANDSHAKE)
K	KEYAGREEMENT	USED IN ECDH HANDSHAKE
D	DECIPHER	USED FOR UNWRAPPING A KEY (E.g. FOR S/MIME DECRYPTION)

FIG. 1b

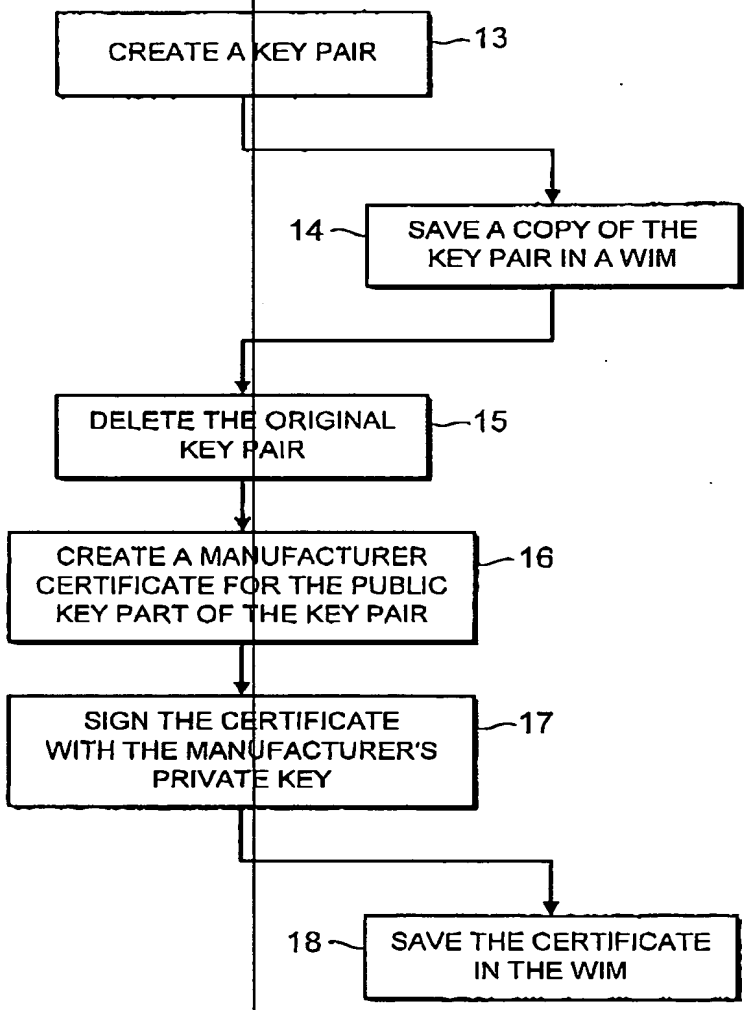

FIG. 2

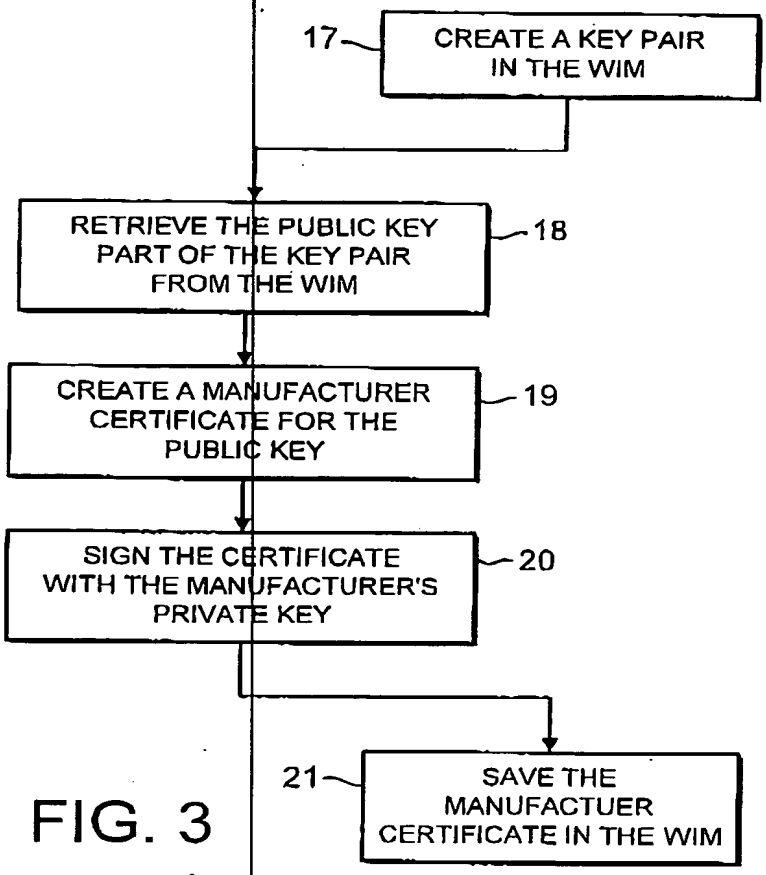

FIG. 3

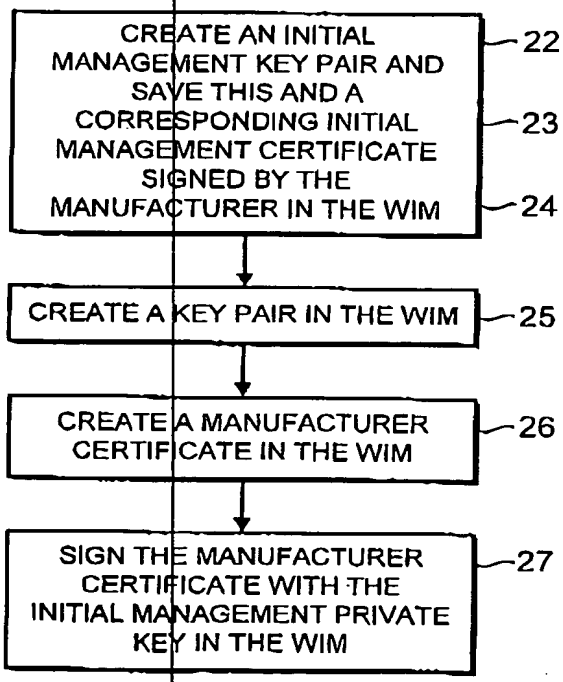

FIG. 4